(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10143695 A**

(43) Date of publication of application: **29.05.98**

(51) Int. Cl **G07B 15/00**
G07B 15/00
G06F 17/60
H04L 9/32

(21) Application number: **08305018**

(22) Date of filing: **15.11.96**

(71) Applicant: **TOSHIBA CORP**

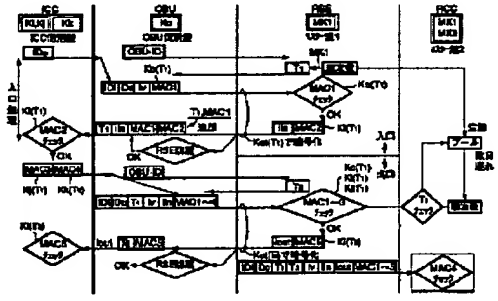
(72) Inventor: **KITAORI MASASHI**
KAWAMURA SHINICHI
FUKAZAWA KAZUO
NAITO KAZUTOSHI

(54) **MUTUAL AUTHENTICATION SYSTEM, TOLL RECEIVING SYSTEM OF TOLL ROAD AND MUTUAL AUTHENTICATION METHOD OF TOLL RECEIVING SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To perform mutual authentication by using a cryptographic key by radio even though the communication speed of an IC card is slow and calculation capability is small and to receive toll by providing an IC read/write device which reads information of an IC card of a facility user and 1st and 2nd authentication devices which are installed at the entrance and exit of the facility.

SOLUTION: Communication between an IC card read/write device which is onboard unit (OBU) that is mounted on a passing vehicle and an entrance roadside system starts. When a passage ticket automatic issuing machine of the entrance roadside system recognizes the OBU, it gives passage permission to the vehicle. The passage ticket automatic issuing machine also sends a message authentication code that makes an IC card recognize as a correct roadside system. An exit traffic lane controller of an exit roadside system confirms a correct OBU, the same OBU at both entrance and exit and a legal IC card by confirming a message authentication code.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－143695

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｂ　15/00	５１０	Ｇ０７Ｂ　15/00	５１０
			Ｂ
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ｃ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｅ

審査請求　未請求　請求項の数８　ＯＬ　（全 17 頁）

(21)出願番号　特願平8－305018

(22)出願日　平成８年(1996)11月15日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　北折　昌司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　深沢　一夫
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

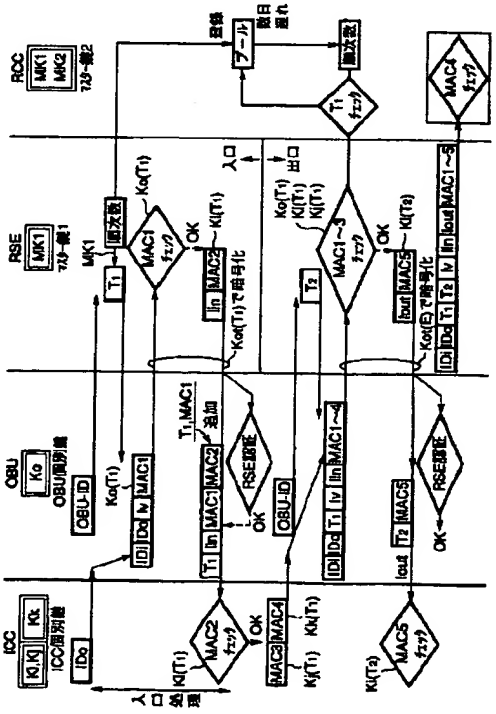
最終頁に続く

(54)【発明の名称】　相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法

(57)【要約】

【課題】ＩＣカードの通信速度が遅く、計算能力が小さくても暗号鍵を用いて無線で相互認証を行って料金の収受を行う。

【解決手段】ＩＣカード（ＩＣＣ）とＯＢＵを介して路側システム（ＲＳＥ）との間で暗号鍵を用いて相互認証を行うが、最初の通過する車両に搭載されているＯＢＵと入口路側システムとの間で通信を開始し、入口路側システムがＯＢＵを確認した時点でこのＯＢＵを搭載した車両の通行が許可され、ＯＢＵを介してＩＣカードにメッセージ認証コードが送信され、今度はＩＣカードが入口路側システムから受け取った入口情報、乱数及びメッセージ認証コードとから入口路側システムの正当性を認証してメッセージ認証コードを生成してＯＢＵに送信し、ＯＢＵと出口路側システムとの間で通信を行って出口路側システムがＯＢＵ、入口情報、ＩＣカードが正当であることを確認する。



1

【特許請求の範囲】

【請求項１】　施設利用者に所有されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される相互認証システムにおいて、

上記第１の認証装置は、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードは、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、

この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

上記第２の認証装置は、

上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、

を具備したことを特徴とする相互認証システム。

【請求項２】　車両に搭載されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される有料道路の料金収受システムにおいて、

上記第１の認証装置は、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報と当該入口を示す入口情報とを上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードは、

ＩＤ番号を含む課金情報を記憶する記憶手段と、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報と入口情報とを受信する第１の受信手段と、

この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

2

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報と入口情報及び上記記憶手段に記憶されている課金情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

上記第２の認証装置は、

上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、

この第２の認証手段により認証できたとき、上記第２の送信手段から送信された入口情報及び課金情報に基づいて有料道路の通行料金の収受処理を行う収受手段と、

を具備したことを特徴とする有料道路の料金収受システム。

【請求項３】　ＩＣカードの情報を読み取り、情報を書き込むＩＣカード読取書込装置と、少なくとも２つの認証装置とから構成される相互認証システムにおいて、

上記ＩＣカード読取書込装置と最初に情報交換を行う第１の認証装置が、

上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、

この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、

上記ＩＣカードが、

上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、

この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、

この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、

この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、

上記第２の認証装置が、

上記第２の送信手段から送信された複数の認証情報による認証を行う第２の認証手段と、

を具備したことを特徴とする相互認証システム。

【請求項４】　車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する入口と出口の路側システムとの間で料金収受が行われる料金収受システムの相互認証方法であって、

上記入口の路側システムがＩＣカード向けの認証情報と

出口の路側システム向けの認証情報とを生成して上記車載機に無線で送信し、上記車載機が送信された２つの認証情報を受信して上記ＩＣカードに送信し、ＩＣカードが送信された２つの認証情報の内のＩＣカード向けの認証情報により認証し、認証された際、上記出口の路側システム向けの認証情報を生成し、生成した出口の路側システム向けの認証情報と上記車載機から送信された２つの認証情報の内の出口の路側システム向けの認証情報とを上記車載機に送信し、上記車載機が送信された２つの認証情報を受信して上記出口の路側システムに無線で送信し、上記出口システムが送信された２つの認証情報により認証するようにしたことを特徴とする料金収受システムの相互認証方法。

【請求項５】　車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、

上記車載機が、

ＩＣカードが挿入された際、乱数を発生する乱数発生手段と、

この乱数発生手段で発生された乱数を上記挿入されたＩＣカードに送信する第１の送信手段と、

上記ＩＣカードが、

上記第１の送信手段から送信された乱数を受信する第１の受信手段と、

この第１の受信手段で乱数が受信された際、予め格納しているＩＤ番号を上記車載機に送信する第２の送信手段と、

上記第１の受信手段で受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化する暗号化手段と、

この暗号化手段で暗号化された暗号文を上記車載機に送信する第３の送信手段と、

上記車載機が、

上記第２の送信手段から送信されたＩＤ番号を受信する第２の受信手段と、

この第２の受信手段で受信されたＩＤ番号から予め格納しているマスタ鍵で秘密鍵を生成する生成手段と、

上記第３の送信手段から送信された暗号文を受信する第３の受信手段と、

この第３の受信手段で受信された暗号文を上記生成手段で生成された秘密鍵で復号化する復号化手段と、

この復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、

この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項６】　車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、

上記車載機がＩＣカードが挿入された際、乱数を発生し、発生された乱数を上記挿入されたＩＣカードに送信し、上記ＩＣカードが送信された乱数を受信し、乱数が受信された際、予め格納しているＩＤ番号を上記車載機に送信し、受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信されたＩＤ番号を受信し、受信されたＩＤ番号から予め格納しているマスタ鍵で秘密鍵を生成し、送信された暗号文を受信し、受信された暗号文を生成された秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする料金収受システムの相互認証方法。

【請求項７】　車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、

上記車載機が、

ＩＣカードが挿入された際、乱数を発生する乱数発生手段と、

この乱数発生手段で発生された乱数と予め格納している車載機固有の公開鍵と対応するディジタル署名とを上記挿入されたＩＣカードに送信する第１の送信手段と、

上記ＩＣカードが、

上記第１の送信手段から送信された乱数と車載機固有の公開鍵と対応するディジタル署名とを受信する第１の受信手段と、

この第１の受信手段で受信された車載機固有の公開鍵と対応するディジタル署名とから予め格納されている公開鍵を用いて復号化する第１の復号化手段と、

この第１の復号化手段で復号化された復号文のディジタル署名が正しいか否かを確認する確認手段と、

この確認手段で正しいと確認された際、上記第１の受信手段で受信された乱数と予め格納されているＩＣカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化する暗号化手段と、

この暗号化手段で暗号化された暗号文を上記車載機に送信する第２の送信手段と、

上記車載機が、

5

上記第２の送信手段で送信された暗号文を受信する第２の受信手段と、
この第２の受信手段で受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化する第２の復号化手段と、
この第２の復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、
この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から上記ＩＣカード固有の秘密鍵を取り出し、このＩＣカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段と、
を具備したことを特徴とする料金収受システム。

【請求項８】　車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、
上記車載機がＩＣカードが挿入された際、乱数を発生し、発生された乱数と予め格納している車載機固有の公開鍵と対応するディジタル署名とを上記挿入されたＩＣカードに送信し、上記ＩＣカードが送信された乱数と車載機固有の公開鍵と対応するディジタル署名とを受信し、受信された車載機固有の公開鍵と対応するディジタル署名とから予め格納されている公開鍵を用いて復号化し、復号化された復号文のディジタル署名が正しいか否かを確認し、正しいと確認された際、受信された乱数と予め格納されているＩＣカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信された暗号文を受信し、受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、上記復号化された復号文から上記ＩＣカード固有の秘密鍵を取り出し、このＩＣカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする料金収受システムの相互認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、例えば有料道路において、車両等の移動体に搭載されている車載機器と無線によって相互認証して料金収受を行う相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法に関する。

【０００２】

【従来の技術】従来、例えば有料道路における料金収受装置の端末装置を備える料金所において、有料道路本線

6

に入線する車両に対して料金所の入口の端末装置で入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行し、上記料金所と有料道路で接続されている他の料金所の出口で、上記料金所で発行された通行券の入口情報により、この料金所の出口に備えられている端末装置を用いて通行料金を計算し、通行料金の収受を行っている。

【０００３】この料金収受装置は、複数の端末装置を持って各料金所に設置されている。料金所の入口の各端末装置は、有料道路本線に入線する車両に対して入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行する。料金所の出口の各端末装置は、通行料金計算のためのテーブル、例えば全ての料金所との区間料金、車種別の料金等をメモリに記憶しており、料金所の出口において料金所の入口で発行された通行券の入口情報によりメモリに記憶している通行料金テーブルを検索して通行料金を計算する。

【０００４】それに対して、車両に搭載した車載機器と地上（料金所）側の通信装置と無線で料金の収受を行う料金収受システムが、非接触、ノンストップのメリットをユーザに提供する手段として注目を受けている。

【０００５】有料道路における無線カード式の料金収受システムの場合、道路側に設置される路側機器と車両に搭載される車載機器との間で無線通信による課金情報の送受信が行われる。ここで、車載機器が支払請求先とは直接関係を持たない車載機と、支払請求先の情報を担ったＩＣカードを用いた構成を想定する。

【０００６】従来、ＩＣカードを使った認証システムでは、通信されたメッセージの所有者（作者）を特定し、かつメッセージが改竄されていないことを確認するためにメッセージ認証コードと呼ばれる符号が使われている。これについて図１３を用いて簡単に説明する。

【０００７】送信者Ａが作ったメッセージは通信手段によって受信者ＢにＡが作成したメッセージとして伝えられたとする。もちろん、この間の送信路に何も問題なければ両者のメッセージは同一であり、また、通信路が一つに確定していればそれはまぎれもなくＡが作ったメッセージであると言える。

【０００８】しかし、一般の通信路ではこの様な保証はなく、誰かがＡを装ってメッセージを作ったり、また、Ａが作ったメッセージを通信過程で何者かが自分の都合の良いように改竄する恐れもある。したがって、Ｂは自分が受け取ったメッセージが確かにＡが作ったものであり、かつ改竄されていないことを確認しなくてはならない。

【０００９】このため送信者Ａと受信者Ｂは、お互いに同じ情報（これを共通鍵と呼ぶ）を共有する。この鍵を用いてＡさんはメッセージをハッシュ関数と呼ばれる関数によってメッセージ認証コード（ＭＡＣ）を作成する。ハッシュ関数は、一方向性関数の一種であり、この

関数の結果から元の値を算出することがきわめて困難な関数である。例えば、ＭＤ５、ＳＨＡと呼ばれるアルゴリズムが良く知られている。

【００１０】Ａはこれをメッセージに添付してＢに送信する。これを受け取ったＢはＡが行ったと同じ行程で同じ共通鍵を使って受け取ったメッセージのメッセージ認証コードを作成する。メッセージが改竄されていれば受け取ったメッセージ認証コードと自分が作成したメッセージ認証コードとが一致しない。また、Ｂが所有する共通鍵を共有するＡ以外にこれと一致するメッセージ認証コードを作成するのは極めて困難であるので、Ｂはこのメッセージの作者がＡであると確認することができる。

【００１１】これはＢがＡのメッセージの正当性を検査する一方向の認証である。さて、ここでＩＣカードがＡであった場合、ＩＣカードを差し込む装置がＢとした場合、もし、このＩＣカードが入退室に使われるならば、つまりＩＣカードを認証する装置が確かにその場所にあるＩＣカードを差し込んだ装置であるならば、認証は一方向で十分である。

【００１２】しかし、ネットワークなどを使った通信を用い、認証する相手が特定できない場合などは、一方向では不十分であり、お互いがお互いを認証しあう相互認証が不可欠である。この場合、メッセージ認証コードを付けたメッセージを相互に交換することで容易に実現できることは明かである。

【００１３】これを図に表すと図１４のようになる。前述の手続きに従って、Ａの要求によりＢはＡの正当性をメッセージ認証コードを検証することで認証する。次に認証結果をＡに返し、ＡがＢの正当性を認証コードを用いて検証する。しかる後に、相互の通信を行うのである。

【００１４】近年、こういったＩＣカードを用いた認証システムが多方面に用いられる試みが行われている。その中には、有料の高速道路の料金収受システムなども含まれる。この場合の料金収受システムの特徴としては、ＩＣカードを搭載した車両が高速道路で入口および出口ゲートを通過する極めて短い時間内にＩＣカードと、高速道路の入口および出口にある路側システムとの相互認証を行う点にある。

【００１５】しかしながら、この相互認証方式を有料道路の料金収受システムなどに応用する場合には次の問題が起きる。まず、Ａすなわちカードは、高速演算が望めないので、Ｂすなわち路側システムの認証を完全に行うことができない。従って、車両が入口の路側システムで相互認証手続きの通信を行って入口の路側システムを認証した結果行われる通信は、次の出口の路側システムまで待機させられる。そして、車両が出口を通過したとき、同様に出口の路側システムを認証する必要が生じ、これにも同様の時間が必要となるため、結局、入口路側システムと出口路側システムを完全に認証した後で

それに基づいた料金収受の通信を行うことが不可能となる。

【００１６】また、路側システムとＩＣカードとの間で容易に考えられる安全な課金方式としては、ＩＣカードに個別の秘密の暗号鍵Ｋが格納されていて、路側システムはあらかじめＩＣカードの識別番号から鍵Ｋを特定し、路側システムが車載機を介してＩＣカードと暗号通信を行うことによって確かに正当なＩＣカードを搭載した車であることを確認するとともに、そのカードから特定される対象者に課金を行うようなシステムがある。ここで、ＩＣカードと路側システムが行う暗号通信とは、例えば次に示す４ステップからなる相互認証プロトコルである。

（１）乱数Ｒ１をＩＣカードが生成し、路側システムに送る。

（２）路側システムは第２の乱数Ｒ２を生成し、Ｒ１とＲ２を連結したものを鍵Ｋで暗号化して、結果をＩＣカードに送る。

（３）ＩＣカードは受信した暗号文を鍵Ｋで復号し、（１）で送ったのと同じＲ１が所定の形式で得られることを確認すると共に、復号文からＲ２を取り出して路側システムに送り返す。

（４）路側システムは送り返された電文が、（２）で生成したＲ２と一致することを確認する。

【００１７】このような手続きの相互認証プロトコルにより路側システムは、ＩＣカードが路側システムと同じ鍵Ｋを持つことが確認できる。鍵Ｋは、カード毎に異なる値を発行するので鍵Ｋが特定できたことにより課金先が特定できたことになる。なお、この手続きが実施できるためには路側システムがＩＣカードと同じ鍵を持つことが必要であるが、路側システムは例えばカードの識別番号とそのカードに格納されている鍵のリストを所持したり、カード識別番号から秘密の変換アルゴリズムによって鍵を導き出す等の手段を用いることができる。

【００１８】このような相互認証の手続きは、用いるＩＣカードが高速の通信機能を有していれば容易に実装できる。しかしながら、ＩＳＯで規格化された標準的なコンタクト型ＩＣカードの通信速度は９．６ｋｂｐｓであり、車両が料金所（入口と出口の路側システム）をノンストップで通過する料金収受システムでは、上記のような相互認証プロトコルをＩＣカードと路側システムとの間で直接行うことはできない。また、仮に通信速度が向上しても、ＩＣカードに搭載されるプロセッサの計算能力は通常小さく、相互認証の暗号化演算をこの時間内で行うことは不可能である。

【００１９】

【発明が解決しようとする課題】上記したように、車両に搭載されるＩＣカードと有料道路の料金所（入口と出口の路側システム）との間で暗号鍵を用いて無線で料金の収受を行なう料金収受システムにおいては、ＩＣカー

9

ドの通信速度が遅いので相互認証をすることができず、また、ＩＣカードの計算能力が小さいので相互認証の暗号化演算を時間内で行うことができないという問題があった。

【００２０】そこで、この発明は、ＩＣカードの通信速度が遅く、計算能力が小さくても暗号鍵を用いて無線で相互認証を行って料金の収受を行うことのできる相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法を提供することを目的とする。

【００２１】

【課題を解決するための手段】この発明の相互認証システムは、施設利用者に所有されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される相互認証システムにおいて、上記第１の認証装置は、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードは、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置は、上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段とから構成されている。

【００２２】この発明の有料道路の料金収受システムは、車両に搭載されるＩＣカードに対して情報の読み取り、及び送信情報を書き込むＩＣカード読取書込装置と、施設の入口に設けられる第１の認証装置と施設の出口に設けられる第２の認証装置とから構成される有料道路の料金収受システムにおいて、上記第１の認証装置は、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報と当該入口を示す入口情報とを上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードは、ＩＤ番号を含む課金情報を記憶する記憶手段と、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報と入口情報とを受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１

10

の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報と入口情報及び上記記憶手段に記憶されている課金情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置は、上記第２の送信手段から送信された複数の認証情報により上記ＩＣカードの認証を行う第２の認証手段と、この第２の認証手段により認証できたとき、上記第２の送信手段から送信された入口情報及び課金情報に基づいて有料道路の通行料金の収受処理を行う収受手段とから構成されている。

【００２３】この発明の相互認証システムは、ＩＣカードの情報を読み取り、情報を書き込むＩＣカード読取書込装置と、少なくとも２つの認証装置とから構成される相互認証システムにおいて、上記ＩＣカード読取書込装置と最初に情報交換を行う第１の認証装置が、上記ＩＣカード向けの認証情報と次に情報交換を行う第２の認証装置向けの認証情報とを生成する第１の生成手段と、この第１の生成手段で生成された２つの認証情報を上記ＩＣカードに送信する第１の送信手段と、上記ＩＣカードが、上記ＩＣカード読取書込装置を介して上記第１の送信手段から送信された２つの認証情報を受信する第１の受信手段と、この第１の受信手段で受信された２つの認証情報の内のＩＣカード向けの認証情報により認証を行う第１の認証手段と、この第１の認証手段により認証された際、上記第２の認証装置向けの認証情報を生成する第２の生成手段と、この第２の生成手段で生成された認証情報と上記第１の受信手段で受信された２つの認証情報の内の第２の認証装置向けの認証情報とを上記ＩＣカード読取書込装置を介して上記第２の認証装置に送信する第２の送信手段と、上記第２の認証装置が、上記第２の送信手段から送信された複数の認証情報による認証を行う第２の認証手段とから構成されている。

【００２４】この発明の料金収受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する入口と出口の路側システムとの間で料金収受が行われる料金収受システムの相互認証方法であって、上記入口の路側システムがＩＣカード向けの認証情報と出口の路側システム向けの認証情報とを生成して上記車載機に無線で送信し、上記車載機が送信された２つの認証情報を受信して上記ＩＣカードに送信し、ＩＣカードが送信された２つの認証情報の内のＩＣカード向けの認証情報により認証し、認証された際、上記出口の路側システム向けの認証情報を生成し、生成した出口の路側システム向けの認証情報と上記車載機から送信された２つの認証情報の内の出口の路側システム向けの認証情報とを上記車載機に送信し、上記車載機が送信された２つの認

11

証情報を受信して上記出口の路側システムに無線で送信し、上記出口システムが送信された２つの認証情報により認証するようにしたことを特徴とする。

【００２５】この発明の料金収受システムは、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、上記車載機が、ＩＣカードが挿入された際、乱数を発生する乱数発生手段と、この乱数発生手段で発生された乱数を上記挿入されたＩＣカードに送信する第１の送信手段と、上記ＩＣカードが、上記第１の送信手段から送信された乱数を受信する第１の受信手段と、この第１の受信手段で乱数が受信された際、予め格納しているＩＤ番号を上記車載機に送信する第２の送信手段と、上記第１の受信手段で受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を上記車載機に送信する第３の送信手段と、上記車載機が、上記第２の送信手段から送信されたＩＤ番号を受信する第２の受信手段と、この第２の受信手段で受信されたＩＤ番号から予め格納しているマスタ鍵で秘密鍵を生成する生成手段と、上記第３の送信手段から送信された暗号文を受信する第３の受信手段と、この第３の受信手段で受信された暗号文を上記生成手段で生成された秘密鍵で復号化する復号化手段と、この復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段とから構成されている。

【００２６】この発明の料金収受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、上記車載機がＩＣカードが挿入された際、乱数を発生し、発生された乱数を上記挿入されたＩＣカードに送信し、上記ＩＣカードが送信された乱数を受信し、乱数が受信された際、予め格納しているＩＤ番号を上記車載機に送信し、受信された乱数と予め格納している相互認証プロトコルに用いる秘密鍵とを予め格納しているカード固有の暗号鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信されたＩＤ番号を受信し、受信されたＩＤ番号から予め格納しているマスタ鍵で秘密鍵を生成し、送信された暗号文を受信し、受信された暗号文を生成された秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、復号化された復号文から相互認証プロトコルに用いる秘密鍵を取り出し、この相互認証プロトコルに用いる秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする。

12

【００２７】この発明の料金収受システムは、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムにおいて、上記車載機が、ＩＣカードが挿入された際、乱数を発生する乱数発生手段と、この乱数発生手段で発生された乱数と予め格納している車載機固有の公開鍵と対応するディジタル署名とを上記挿入されたＩＣカードに送信する第１の送信手段と、上記ＩＣカードが、上記第１の送信手段から送信された乱数と車載機固有の公開鍵と対応するディジタル署名とを受信する第１の受信手段と、この第１の受信手段で受信された車載機固有の公開鍵と対応するディジタル署名とから予め格納されている公開鍵を用いて復号化する第１の復号化手段と、この第１の復号化手段で復号化された復号文のディジタル署名が正しいか否かを確認する確認手段と、この確認手段で正しいと確認された際、上記第１の受信手段で受信された乱数と予め格納されているＩＣカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を上記車載機に送信する第２の送信手段と、上記車載機が、上記第２の送信手段で送信された暗号文を受信する第２の受信手段と、この第２の受信手段で受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化する第２の復号化手段と、この第２の復号化手段で復号化された復号文の所定の位置に上記乱数発生手段で発生された乱数と同じ乱数があるか否かを確認する確認手段と、この確認手段で同じ乱数が確認された際、上記復号化手段で復号化された復号文から上記ＩＣカード固有の秘密鍵を取り出し、このＩＣカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御する制御手段とから構成されている。

【００２８】この発明の料金収受システムの相互認証方法は、車両に設けられた車載機とこの車載機に挿入されるＩＣカードとから構成される車載機器と、上記車両が通過する路側システムとの間で無線によって料金収受が行われる料金収受システムの相互認証方法であって、上記車載機がＩＣカードが挿入された際、乱数を発生し、発生された乱数と予め格納している車載機固有の公開鍵と対応するディジタル署名とを上記挿入されたＩＣカードに送信し、上記ＩＣカードが送信された乱数と車載機固有の公開鍵と対応するディジタル署名とを受信し、受信された車載機固有の公開鍵と対応するディジタル署名とから予め格納されている公開鍵を用いて復号化し、復

13

号化された復号文のディジタル署名が正しいか否かを確認し、正しいと確認された際、受信された乱数と予め格納されているＩＣカード固有の秘密鍵とを連結して上記復号文の車載機固有の公開鍵で暗号化し、暗号化された暗号文を上記車載機に送信し、上記車載機が送信された暗号文を受信し、受信された暗号文を上記車載機固有の公開鍵に対応する車載機固有の秘密鍵で復号化し、復号化された復号文の所定の位置に上記発生された乱数と同じ乱数があるか否かを確認し、同じ乱数が確認された際、上記復号化された復号文から上記ＩＣカード固有の秘密鍵を取り出し、このＩＣカード固有の秘密鍵を用いて上記路側システムとの間で相互認証プロトコルを制御するようにしたことを特徴とする。

【００２９】

【発明の実施の形態】以下、この発明の一実施例について図面を参照して説明する。この発明に係る料金収受システムは、入口と出口の路側システムから構成される入口発券出口収受方式（以下、クローズドシステムと記述する）と、均一車線のみで構成されるオープンシステムとに分けられる。

【００３０】また、詳しくは後述するが車両に搭載される車載機器は、無線通信機能や操作部、表示部を備えた車載機としてのオンボードユニット（On Board Unit：以下、ＯＢＵと記述する）２と利用者のＩＤ番号、口座番号（以下、課金情報と記述する）を備えたＩＣカード１とから構成されている。

【００３１】また、ＯＢＵ２には、予め搭載する車両の車種を決定する要因の長さ・軸数・重量・用途・特長のデータ（以下、車両情報と記述する）が登録されている。ＩＣカード１には、課金情報が記憶されている。

【００３２】図１は、この発明の料金収受システムに係るＩＣカード１の構成を示すものである。すなわち、ＩＣカード１は、全体の制御を司るＣＰＵ１０、制御プログラム等を記憶しているＲＯＭ１１、課金情報等を記憶するＲＡＭ１２、乱数を発生する乱数発生器１３、後述するセキュリティ方式Ａまたセキュリティ方式Ｂのための鍵が格納される鍵格納エリア１４、及び暗号化アルゴリズム実行器１５とから構成されている。

【００３３】図２は、ＯＢＵ２の構成を示すものである。すなわち、ＯＢＵ２は、全体の制御を司るＣＰＵ２０、制御プログラム等を記憶しているＲＯＭ２１、車両情報等を記憶するＲＡＭ２２、乱数を発生する乱数発生手段としての乱数発生器２３、後述するセキュリティ方式Ｂのための鍵が格納される鍵格納エリア１４、暗号化アルゴリズム実行器１５、各車線に設置されたアンテナと交信を行うアンテナ２６、アンテナ２６の制御を行う無線通信制御部２７、操作案内をする文字表示とＬＥＤランプを備えた表示部２８、複数のボタンを備えた操作部２９、及びＩＣカード１が装着されて読取り・書込みが可能なＩＣカード処理部１８とから構成されている。

14

【００３４】図３は、路側システム（ＲＳＥ）として、クローズドシステムに用いられる入口路側システムの構成を示すものである。すなわち、入口路側システムは、車両の進行方向から車種判別装置３１、第１アンテナ３２、通行券自動発行機３０、発進検知装置３３、及び第２アンテナ３４とから構成されている。

【００３５】車種判別装置３１は、進入した車両を検知し、車両の進入を通行券自動発行機３０に伝達する。さらに、進入した車両の車種を判別し、判定結果を通行券自動発行機３０に通知する。

【００３６】第１アンテナ３２は、通行券自動発行機３０の指示により、進入した車両に搭載された車載機器との通信を行うものである。発進検知装置３３は、車両の発進を検知し、通行券自動発行機３０に通知する。

【００３７】第２アンテナ３４は、第１アンテナ３２で正常に交信が終了した車両が発進検知装置３３に進入することにより、通行券自動発行機３０の指示の元で、車載機器との通信を行うものである。

【００３８】通行券自動発行機３０は、各機器の制御を行うと同時に、車載機器を搭載していない車両（以下、非ＥＴＣ車と記述する）に対して通行券を発行する。通行券自動発行機３０にはネガティブリストが登録されている。

【００３９】図４は、路側システム（ＲＳＥ）として、クローズドシステムに用いられる出口路側システムの構成を示すものである。図４の（ａ）に示すように出口路側システムは、車両の進行方向から車両検知装置４１、第１アンテナ４２、出口ブース内機器４３、車両検知装置４４、及び第２アンテナ４５とから構成されている。

【００４０】出口ブース内機器４３は、図４の（ｂ）に示すように非ＥＴＣ車が持参した通行券を処理する通行券確認機４６、前納のカードを処理するカード処理機４７、現金支払い車に対する領収書発行を行う領収書発行機４８、各機器の制御を行う出口車線制御装置４０とから構成されている。出口車線制御装置４０は、ネガティブリストが登録されている。なお、通行券確認機４６は、ＩＣカード１を処理することのできるＩＣカードリーダ４６ａを備えている。

【００４１】車両検知装置４１は、車両の進入を検知した結果を出口ブース内機器４３の出口車線制御装置４０に通知する。第１アンテナ４２は、出口車線制御装置４０の制御の元で、進入車両に搭載された車載機器との交信を行うものである。

【００４２】車両検知装置４４は、車両の進入を検知した結果を出口車線制御装置４０に通知する。第２アンテナ４５では、出口車線制御装置４０の制御の元で、車両に搭載された車載機器との交信を行う。

【００４３】図５は、路側システム（ＲＳＥ）として、オープンシステムに用いられる均一路側システムの構成を示すものである。図５の（ａ）に示すように均一路側

15

システムは、車両の進行方向から車両検知装置５１、第１アンテナ５２、ブース内機器５３、車両検知装置５４、及び第２アンテナ５５とから構成されている。

【００４４】ブース内機器５３は、図５の（ｂ）に示すように料金支払種別や進入車両の車種を入力し、各機器の制御を行う料金処理機５０、前納のカードを処理するカード処理機５６、現金支払い車に対する領収書の発行を行う領収書発行機５７、ＩＣカード１を処理することのできるＩＣカードリーダ５８とから構成されている。なお、料金処理機５０にはネガティブリストが登録されている。

【００４５】車両検知装置５１は、車両の進入を検知した結果をブース内機器５３の料金処理機５０に通知する。第１アンテナ５２は、料金処理機５０の制御の元で、進入車両に搭載された車載機器との交信を行うものである。

【００４６】車両検知装置５４は、車両の進入を検知した結果を料金処理機５０に通知する。第２アンテナ５５では、料金処理機５０の制御の元で、車両に搭載された車載機器との交信を行う。

【００４７】利用者は、車両に車載機器を搭載し、ＯＢＵ２にＩＣカード１を挿入した状態で走行する。ＯＢＵ２に挿入されたＩＣカード１は、ＯＢＵ２の正当性を確認することにより、ＯＢＵ２に対してカードＩＤ番号を通知する。

【００４８】次に、クローズシステムの道路を利用する例について説明する。入口路側システムでは、車種判別装置３１が車両の進入を検知することにより、通行券自動発行機３０に進入検知を伝達する。通行券自動発行機３０は、第１アンテナ３２を制御し、進入する車両に搭載されている車載機器（ＩＣカード１が挿入されたＯＢＵ２）に対する交信問い合わせを開始する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めＩＣカード１から通知されたＩＤ番号とＯＢＵ２に記録されている車両情報を返信する。

【００４９】通行券自動発行機３０は、車載機器からの応答が正当と認識することにより、ＩＣカード１のＩＤ番号をネガティブリストと照合し、正当であれば入口を特定する道路番号・料金所番号・通過年月日時分・車線番号（以下、入口情報Ａと記述する）を車載機器に送信する。ＯＢＵ２では、入口情報Ａの受信が正常に行われたことを確認して、入口路側システムに受信完了を通知する。

【００５０】入口路側システムは、車載機器からの受信完了を受けることにより、通行券自動発行機３０に発券停止を指示し、正常な車載機器搭載車両（以下、ＥＴＣ車と記述する）と認定する。

【００５１】ＥＴＣ車が発信検知装置３３を通過することにより、通行券自動発行機３０は、発信検知装置３３から車両進入の通知を受け、第２アンテナ３４を制御し、車載機器に対する交信問い合わせを実行する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めＩＣカード１から通知されたＩＤ番号を通知する。

16

【００５２】通行券自動発行機３０は、車載機器からの応答が正当と認識することにより、ＩＣカード１のＩＤ番号を第１のアンテナ３２で受信したものと比較し、一致していれば車種判別装置３１から受信した車種判定結果を入口情報Ｂとして第２アンテナ３４を利用して車載機器に返信する。

【００５３】車載機器（ＩＣカード１が挿入されたＯＢＵ２）では、入口情報Ｂのデータが正常に受信されたことを確認し、第２アンテナ３４に受信完了を通知する。同時に車載機器では、正常に受信した入口情報Ａと入口情報ＢとをＩＣカード１に入口情報（入口情報Ａと入口情報Ｂとを合わせたものを入口情報とする）として記録する。

【００５４】出口路側システムでは、車両検知装置４１が車両の進入を検知することにより、車両の進入を出口車線制御装置４０に通知する。出口車線制御装置４０では、第１アンテナ４２を制御し、進入した車両に対して問い合わせを実行する。出口路側システムでも入口路側システム同様に相手の正当性を認識することにより、車載機器は、ＯＢＵ２に記録されている入口情報及び課金情報を第１アンテナ４２に伝送する。

【００５５】出口車線制御装置４０では、第１アンテナ４２を経由して受信した入口情報を元に通行料金の算出を行い、同時にＩＤ番号のネガティブリスト照合を行い、ＩＤ番号の正当性を認識することにより、入口情報及び出口情報（料金所番号・通過年月日時分・車線番号・通行料金）を利用履歴として、ＯＢＵ２に伝送する。ＯＢＵ２では、利用履歴が正常に受信完了したことを確認し、路側システムに受信完了を通知する。同時に、ＩＣカード１に対して利用履歴を記録する。

【００５６】次に、オープンシステムの均一路側システムについて説明する。上述したクローズシステムと同様に利用者は、車両に車載機器を搭載し、ＯＢＵ２にＩＣカード１を挿入した状態で走行する。ＩＣカード１は、ＯＢＵ２の正当性確認を行い、ＩＤ番号を通知しておく。

【００５７】均一路側システムでは、車両検知装置５１が車両の進入を検知することにより、料金処理機５０に車両進入を通知する。料金処理機５０は、第１アンテナ５２を制御し、車載機器に対して問い合わせを実行する。上述した入口車線と同様に相手の正当性を認識することにより、ＯＢＵ２は、予め通知されたＩＣカード１のＩＤ番号とＯＢＵ２に記録された車両情報を第１アンテナ５２に送信する。

【００５８】料金処理機５０では、第１アンテナ５２を経由して受信したＩＤ番号をネガティブリストと照合

し、正当性が認識された場合、車両情報を元にした車種判定が行われ、判定した車種で通行料金を算出する。算出結果を元に料金所情報（料金所番号・通過年月日時分・車線番号・通行料金）を生成し、利用履歴としてＯＢＵ２に伝送する。

【００５９】ＯＢＵ２では利用履歴が正常に受信完了したことを確認し、均一路側システムに受信完了を通知する。同時に、ＩＣカード１に対して利用履歴を記録する。図６は、この発明に係る通行券自動発行機３０の構成を示すものである。すなわち、通行券自動発行機３０は、各機器と接続されて全体の制御を司るＣＰＵ３０１、制御プログラム等を記憶しているＲＯＭ３０２、各種情報を記憶するＲＡＭ３０３、乱数を発生する乱数発生器３０４、後述するセキュリティ方式Ａのための鍵が格納される鍵格納エリア３０５、暗号化アルゴリズム実行器３０６、及び通行券発行処理部３０７とから構成されている。

【００６０】図７は、この発明に係る出口車線制御装置４０の構成を示すものである。すなわち、出口車線制御装置４０は、各機器と接続されて全体の制御を司るＣＰＵ４０１、制御プログラム等を記憶しているＲＯＭ４０２、各種情報を記憶するＲＡＭ４０３、乱数を発生する乱数発生器４０４、後述するセキュリティ方式Ａのための鍵が格納される鍵格納エリア４０５、及び暗号化アルゴリズム実行器４０６とから構成されている。

【００６１】次に、このような構成において第１実施例について説明する。まず、利用者は車両に車載機器を搭載し、ＯＢＵ２にＩＣカード１を挿入した状態で走行する。ＩＣカード１の鍵格納エリア１４には、登録発行時に特定の数字（ＩＣ－ＩＤ）および３つの個別鍵（Ｋｉ、Ｋｊ、Ｋｋ）が格納されている。ＫｉおよびＫｊは、ＩＣ－ＩＤに路側システム固有鍵ＭＫ１を一方向性関数を用いて作用させることによって生成する。

【００６２】

Ｋｉ＝ｆ（ＩＣ－ＩＤ、ＭＫ１）……（１）

ただしｆ（）は一方向性関数。

Ｋｊ＝ｇ（ＩＣ－ＩＤ、ＭＫ１）……（２）

ただしｇ（）は一方向性関数。

【００６３】また、ＫｋはＩＣ－ＩＤにカード発行局固有鍵ＭＫ２を一方向性関数を用いて作用させることによって、Ｋｉ、Ｋｊ同様に生成する。

Ｋｋ＝ｈ（ＩＣ－ＩＤ、ＭＫ２）……（３）

ただしｈ（）は一方向性関数。

【００６４】一方向性関数を用いることによって、ＩＣカード１に格納されるＫｉ、ＫＪ、Ｋｋが不正に読まれたとしても、これらを導き出すのに用いられたシステム固有鍵ＭＫ１、ＭＫ２を逆算により求めることは不可能となるので本システム全体の安全性は保たれる。

【００６５】ＯＢＵ２にもまた特定の数字（ＯＢＵ－ＩＤ）と２つの個別鍵（Ｋ０、Ｋ０ｔ）が鍵格納エリア２４に格納されている。Ｋ０はＩＣカード１の個別鍵同様、ＯＢＵ－ＩＤに路側システム固有鍵ＭＫ１を一方向性関数を用いて作用させたことによって生成する。

【００６６】

Ｋ０＝Ｆ（ＯＢＵ－ＩＤ、ＭＫ１）……（４）

ただし、Ｆ（）は一方向性関数。一方、Ｋ０ｔは全てのＯＢＵ２に共通していて、路側システムにも与えられる情報であり、おもに通信路の暗号化鍵生成に用いられる。Ｋ０、Ｋ０ｔ共に、それ自体はＩＣチップの中に埋め込まれるか、あるいは既知の物理的手段によって、プローブ等で取り出すことが出来ないように保護されている。

【００６７】ＩＣカード１をＯＢＵ１に差し込んだとき、あるいはＩＣカード１を差し込んだ後にＯＢＵ２に電源が投入されたとき、あるいはＩＣカード１を差し込んだ後にＯＢＵ２の所定のスイッチもしくは所定の複数キーを入れたとき、あるいはＯＢＵ２が路側システムから所定の信号を受け取ったとき、ＩＣカード１のＩＣ－ＩＤがＯＢＵ２に送信され格納される。

【００６８】その後、ＩＣ－ＩＤは、ＯＢＵ２の電源が切断されたとしても既知のバックアップ手段によりＯＢＵ２内に保持される。付加機能として、ＯＢＵ２にＩＣ－ＩＤ情報の抹消を行う手段を設けること、およびバックアップの時間制限機能を設け、例えば電源切断状態が１日連続すればＩＣ－ＩＤ情報を抹消するといった設定を可能とするのも有効である。

【００６９】次に、車両が路側システム（ＲＳＥ）の入口に達したときのＯＢＵ２と路側システム（ＲＳＥ）との情報の流れを図８を参照して説明する。まず、最初に通過する車両に搭載されているＯＢＵ２と入口路側システムとの通信が開始される。

【００７０】ＯＢＵ２からＯＢＵ－ＩＤが入口路側システムの通行券自動発行機３０に送信され、続いて通行券自動発行機３０からＯＢＵ２に疑似乱数（Ｔ１）が送信される。疑似乱数は、順次数もしくは時刻を示す数を路側システム固有鍵ＭＫ１で暗号化して生成される。使われた順次数もしくは時刻を示す数はホストとしてのＩＣカード発行局（ＲＣＣ）に通知される。

【００７１】ＯＢＵ２は、Ｔ１及びＫ０からセッション鍵Ｋ０（Ｔ１）を所定の関数を用いて生成する。ＯＢＵ２は、ＩＣカード１から受け取り保持しているＩＣ－ＩＤと、ＯＢＵ２が格納しているＯＢＵ－ＩＤおよび車両情報（Ｉｖ）について、Ｋ０（Ｔ１）を用いてメッセージ認証コード（ＭＡＣ１）を生成する。

【００７２】

ＭＡＣ１＝ＭＡＣ（Ｋ０（Ｔ１）、ＩＣＣ－ＩＤ、ＯＢＵ－ＩＤ、Ｉｖ）…………（５）

19

ただし、ＭＡＣ（ｋ、｜Ｉ｜）はメッセージＩについてｋを鍵としたメッセージ認証関数である。

【００７３】さらにＯＢＵ２は、Ｔ１及びＫ０ｔから通信のためのセッション鍵Ｋ０ｔ（Ｔ１）を所定の関数を用いて生成する。ＩＣ－ＩＤ、ＯＢＵ－ＩＤ、Ｉｖ、及びＭＡＣ１はＫ０ｔ（Ｔ１）を鍵として暗号化され、通行券自動発行機３０に送信される。

【００７４】通行券自動発行機３０では、ＯＢＵ２から受け取ったＯＢＵ－ＩＤと路側システム固有鍵ＭＫ１から式４を用いてＫ０を算出すると共に、全てのＯＢＵ２に共通なＫ０ｔとＯＢＵ２に送信したＴ１から所定の関数によりＫ０ｔ（Ｔ１）を算出する。受け取った情報はＫ０ｔ（Ｔ１）を鍵として暗号化されているので、路側システムの通行券自動発行機３０はこれを直ちに解いて情報を取り出すことができる。

【００７５】つぎに通行券自動発行機３０は、ＯＢＵ２が付けたＭＡＣ１を検証する。これには、ＯＢＵ２が行ったと同様の手続きをセッション鍵Ｋ０ｔ（Ｔ１）を用いてメッセージ認証コードを生成し、これとＯＢＵ２から受け取ったＭＡＣ１とが一致することを確認する。一致していれば、メッセージすなわちＩＣ－ＩＤ、ＯＢＵ－ＩＤ、Ｉｖが全て正しい情報であることが確認できると共に、メッセージ認証に用いたセッション鍵が、通行券自動発行機３０がその場で生成した乱数Ｔ１に基づい＊

20

＊て作られているので、入口にさしかかったＯＢＵ２がメッセージ認証コードを正しく生成したと言うことが確認できる。これはメッセージが盗聴などされ時間差を置いて２度使われるという、いわゆるリプレイ攻撃を阻止するのに非常に重要なポイントである。そしてこれによって通行券自動発行機３０はＯＢＵ２を認証することができるのである。

【００７６】通行券自動発行機３０がＯＢＵ２を認証した時点で、ＯＢＵ２を搭載した車両は通行許可が与えられる。しかし、通行券自動発行機３０はＯＢＵ２へ正しい入口情報を送信しなければならないし、また、決済を行うＩＣカード１に対して自分が正しい路側システムであることを認証させるためにＩＣカード１の鍵に基づくメッセージ認証コードを送信しなければならない。

【００７７】このため、ＯＢＵ２から受け取ったメッセージが正しいことが確認できると、路側システムの通行券自動発行機３０は、ＩＣ－ＩＤと路側システム固有鍵ＭＫ１から式１に基づきＩＣカード固有鍵の一つＫｉを生成する。さらにＫｉと乱数Ｔ１から所定の関数からＫｉ（Ｔ１）を生成する。そして入口情報（Ｉｉｎ：入口名称、時刻、車両情報など）およびＭＡＣ１についてＫｉ（Ｔ１）を用いてメッセージ認証コード（ＭＡＣ２）を生成する、

$$MAC2=MAC(Ki(T1)、MAC1、Iin) \quad \cdots\cdots (6)$$

※ＯＢＵ２では確認されないがＩＣカード１の中で確認され、その情報が出口路側システムで確認されるため、こういった不正は必ず出口で検出できる。

【００８０】次に、ＩＣカード１内での処理と出口処理について説明する。正しい路側システムとして入口路側システム（通行券自動発行機３０）から受け取った入口データ（Ｉｉｎ）、乱数（Ｔ１）及びメッセージ認証コード（ＭＡＣ２）は、ＩＣカード１とＯＢＵ２間の所定のインターフェースを通ってＩＣカード１へ送られる。ＭＡＣ２は、路側システム（通行券自動発行機３０）がＩＣカードの個別鍵Ｋｉを用いて作成したコードである。従って、ＩＣカード１は路側システムと同様の手続きで、個別鍵Ｋｉを用いてメッセージ認証コードを作成し、これをＭＡＣ２と比較する。一致すれば、この入口情報はＩＣカード１の個別鍵を知り得る正当な路側システムが作った情報であることが確認でき、これによってＩＣカードは路側システムを認証できる。

【００８１】続いてＩＣカード１は、ＭＡＣ２に対して二つの個別鍵Ｋｊ、Ｋｋと乱数Ｔ１を用いてそれぞれメッセージ認証コード（ＭＡＣ３およびＭＡＣ４）を生成し、これをＯＢＵ２に送信する。

【００８２】

$$MAC3=MAC(Kj(T1)、MAC2) \quad \cdots\cdots (7)$$

ただし、ＭＡＣ（ｋ、｜Ｉ｜）はメッセージＩについてｋを鍵としたメッセージ認証関数である。

【００８３】

$$MAC4=MAC(Ki(T1),MAC3)\quad\cdots\cdots\cdots\cdots\quad(8)$$

ただし、MAC（k、｜I｜）はメッセージIについてkを鍵としたメッセージ認証関数である。

【００８４】ＯＢＵ２はこれを出口まで保持する。もちろんこれらの情報についても、ＩＣ－ＩＤの保持に用いるバックアップ機能及び、バックアップ制限機能は有効に作用し、ＩＣカード１を抜いても、ＯＢＵ２の電源が遮断されても情報は失われることはないし、またあらかじめ設定した時間に達したり、所定の操作によって情報を消去することも可能である。

【００８５】出口では、まずＯＢＵ２はＯＢＵ固有値（ＯＢＵ－ＩＤ）を出口路側システム（ＲＳＥ）の出口車線制御装置４０に送信し、出口車線制御装置４０はＯＢＵ２に疑似乱数Ｔ２を送信する。ＯＢＵ２は、所定の関数により暗号通信のためのセッション鍵Ｋ０ｔ（Ｔ２）を生成する。続いてＯＢＵ２は、ＩＣカード固有値（ＩＣ－ＩＤ）、ＯＢＵ固有値（ＯＢＵ－ＩＤ）、疑似乱数（Ｔ１）、およびこれまで用いた全てのメッセージ認証コード（ＭＡＣ１、ＭＡＣ２、ＭＡＣ３、ＭＡＣ４）を、Ｋ０ｔ（Ｔ２）を鍵として暗号化し、出口車線制御装置４０に送信する。

【００８６】出口車線制御装置４０では、Ｋ０ｔ（Ｔ２）を鍵として暗号を解いた後、４つのメッセージ認証コードの内３つを一つ一つ確認する。まず、ＭＡＣ１を確認することでＯＢＵ２がＯＢＵ個別鍵Ｋ０をもつ正当なＯＢＵ２であることと、入口および出口で同じＯＢＵ２であることを確認する。続いて、ＭＡＣ２を確認することで入口情報が改竄された情報でなく正当な路側システムにおける入口路側システムの通行券自動発行機３０が生成した情報であることを確認する。さらに、ＭＡＣ３を確認することで、この入口情報が路側システム（通行券自動発行機３０）が認識したＩＣカード１が、入口通過中または直後にＯＢＵ２に挿入されていたことを確認する。

【００８７】全てが正しく認証されるとＯＢＵ２は、疑似乱数Ｔ１の元になった順次数もしくは時間数を、路側システム固有鍵ＭＫ１を鍵として複号することによって得る。路側システム（ＲＳＥ）において、入口路側システムの通行券自動発行機３０からＩＣカード発行局（ＲＣＣ）へ登録された順次数は、数日間の後れをもって出口路側システムの出口車線制御装置４０に配送されＲＡＭ４０３にテーブル化されている。

【００８８】出口車線制御装置４０がＲＡＭ４０３のテーブルを参照し、もしＴ１がこのテーブル上にあれば、ＯＢＵ２が出口路側システムの出口車線制御装置４０に送信した情報は不自然に古い、すなわち入口から出口に達するまで異常と推定できる時間を要していると判断できるので、この情報は不正にコピーされ再利用されていると考えられるので、その場合は認証できないものとして、本システム以外の所定の手続きにまわることになる。

【００８９】認証が終了すると出口車線制御装置４０は、所定のプログラムにより金額を決定し、この課金情報およびＯＢＵ２から受け取った全ての情報をＩＣカード発行局（ＲＣＣ）へ送信する。

【００９０】続いて、出口車線制御装置４０は、ＫｉとＴ２から所定の関数によりＫｉ（Ｔ２）を計算し、これを鍵として課金情報にメッセージ認証コード（ＭＡＣ５）を生成し、ＯＢＵ２にＫ０ｔ（Ｔ２）を鍵として暗号化し送信する。

【００９１】ＯＢＵ２は、受け取った情報をＫ０ｔ（Ｔ２）を鍵として複号化し、入口同様正しく復号できれば正当な路側システム（出口車線制御装置４０）として認証できる。そして受け取った情報をＩＣカード１に送信する。ＩＣカード１は、課金情報に付けられたメッセージ認証コード（ＭＡＣ５）により、出口車線制御装置４０からの情報の正当性を検証し、認証できれば課金情報をログとしてＩＣカード１内に保管する。

【００９２】さて、ＩＣカード発行局（ＲＣＣ）では，出口路側システムの出口車線制御装置４０から受け取った情報を全てのメッセージ認証コードを検証することによりチェックし、所定金融機関に対して課金通知を行うとともに、疑似乱数生成に使用した順次数または時刻数を登録する。これらは一度使用されたものであるので二度と使用されてはいけないものである。したがつて使用済みとして登録された順次数は速やかに路側システムにおける各出口路側システムの出口車線制御装置４０にネガティブリストとして配布される。これにより、情報の不正な二重使用を実質的に排除することができる。

【００９３】次に、第２実施例について説明する。第２実施例における方式は、路側システムの料金所（入口路側システム）進入前に、事前にＯＢＵ２にＩＣカード１の課金情報を送信が可能な方式で以下に説明する。この時、ＩＣカード１とＯＢＵ２との間の通信路を保護しておかなければＩＣカード固有の秘密の鍵Ｋが第三者に知られる可能性が非常に高くなる。そこで、本発明は、ＩＣカード１とＯＢＵ２との間の通信路を保護し、ＩＣカード固有の鍵ＫをＯＢＵ２に安全に転送する手段が最も重要である。

【００９４】ここで、以下に考えられるいくつかの方法を提示する。

（１）ＩＣカードをＯＢＵに取り込み、データの送受信中は取り出せないようにする。

（２）秘密鍵を用いる方式

（３）公開鍵を用いる方式

上記（１）の方式については既知の技術で対応可能である。

23

【００９５】次に、（２）の秘密鍵を用いる方式について説明する。図９は、発行局におけるＩＣカード発行時の秘密鍵を示すものである。すなわち、あらかじめＩＣカード１には、カード発行時にカードＩＤ番号からマスター鍵ＫＭと所定の秘密鍵暗号アルゴリズムに基づいて導き出された鍵ＫｉがＩＣカード１の鍵格納エリア１４に記憶されている。さらにＩＣカード１には、前記鍵Ｋｉとは異なる相互認証プロトコルに用いるための鍵Ｋａｎｓとが鍵格納エリア１４に記憶されている。ＯＢＵ２にも外部からは読めない形で共通のマスター鍵ＫＭが鍵格納エリア２４に記憶されている。

【００９６】ＯＢＵ２のＣＰＵ２０では、ＩＣカード処理部１８でＩＣカード１の挿入を検知することにより、ＩＣカード１とのデータ送受信を開始するが、データ送受信を行う前にセキュリティ上は相互認証を行う必要がある。

【００９７】そこで、ＯＢＵ２とＩＣカード（ＩＣＣ）１との相互認証動作を図１０を参照して説明する。まず、ＯＢＵ２のＣＰＵ２０は、乱数発生器２３により乱数Ｒ１を発生させ、これをＩＣカード１に送信する。また、ＩＣカード１のＣＰＵ１０は、鍵格納エリア１４に記憶されているＩＤ番号をＯＢＵ２に送信する。

【００９８】さらにＩＣカード１のＣＰＵ１０は、鍵格納エリア１４に記憶されているＩＤ番号及び鍵Ｋａｎｓと乱数Ｒ１を連結してこれを鍵Ｋｉで暗号化アルゴリズム実行器１５を用いて暗号化し、この暗号文Ｋ（Ｒ１＋Ｋａｎｓ）をＯＢＵ２に送信する。

【００９９】ＯＢＵ２のＣＰＵ２０は、受信したＩＤ番号からマスター鍵ＫＭと所定の秘密鍵暗号アルゴリズムに基づいて暗号化アルゴリズム実行器２５で鍵Ｋｉを生成し、Ｋｉを用いてＩＣカード１から受信した暗号文Ｋ（Ｒ１＋Ｋａｎｓ）を復号化する。ＣＰＵ２０は、復号文の所定の位置にＩＣカード１に送信した乱数と同じ乱数が存在することを確認する。もし同じ乱数が確認できなければ、ＯＢＵ２のＣＰＵ２０は処理ＮＧとする。

【０１００】同じ乱数が確認された後、ＯＢＵ２のＣＰＵ２０は、鍵Ｋａｎｓが正しく受信できたものとして復号文から鍵を取り出し、その鍵を用いて路側システムとの間で相互認証プロトコルを実施する。

【０１０１】次に、（３）の公開鍵を用いる方式について説明する。まず、ＩＣカード１は、鍵Ｋと本方式に共通の公開鍵ＰＫがＩＣカード発行時点でＩＣカード１の鍵格納エリア１４に記憶されている。

【０１０２】図１１は、発行局におけるＯＢＵ２発行時の暗号鍵を示すものである。すなわち、ＯＢＵ２には、ＯＢＵ固有の秘密鍵ＳＫｓと秘密鍵と対をなす公開鍵ＰＫｓとが鍵格納エリア２４に記憶されている。また、この公開鍵ＰＫｓには、本方式に共通の秘密鍵ＳＫでディジタル署名ＤＳｓが付けられている。ＯＢＵ固有の秘密鍵ＳＫｓは、外部から読めない形で記憶されている。

24

【０１０３】ここで、ＯＢＵ２とＩＣカード（ＩＣＣ）１との相互認証動作を図１２を参照して説明する。まず、ＯＢＵ２のＣＰＵ２０は、乱数発生器２３により乱数を生成し、これと鍵格納エリア２４に記憶したＯＢＵ固有の公開鍵ＰＫｓと対応するディジタル署名ＤＳｓをＩＣカード１に送る。

【０１０４】ＩＣカード１のＣＰＵ１０は、まず、添付されてきたディジタル署名が正しいものであることを本方式に共通の公開鍵ＰＫで確認する（復号化）。ＰＫｓ＝ＰＫｓが確認できなかった場合は処理ＮＧとして異常終了する。ＰＫｓ＝ＰＫｓが確認できてＯＢＵ２の正当性の確認が完了した場合、ＣＰＵ１０は、鍵Ｋと乱数Ｒ１を連結して、これをＯＢＵ固有の公開鍵ＰＫｓで暗号化アルゴリズム実行器２５を用いて暗号化し、暗号文ＰＫｓ（Ｒ１＋Ｋ）をＯＢＵ２に送信する。

【０１０５】ＯＢＵ２のＣＰＵ２０は、この暗号文ＰＫｓ（Ｒ１＋Ｋ）をＯＢＵ固有の秘密鍵ＳＫｓで復号化し、所定の場所にＯＢＵ２が送信したものと同じ乱数Ｒ１が記録されていることを確認する。Ｒ１＝Ｒ１が確認できなかった場合、ＣＰＵ２０は処理ＮＧとする。

【０１０６】Ｒ１＝Ｒ１が確認できて完了した場合、ＯＢＵ２のＣＰＵ２０は、鍵Ｋが正しく受信完了したものとして復号文から鍵Ｋを取り出し、その鍵Ｋを用いて路側システムとの間で相互認証プロトコルを実施する。

【０１０７】以上説明したように上記発明の実施の形態によれば、第１実施例では、ＩＣカードの処理能力不足を補うため、入口と出口の路側システムの間で時間的な余裕を生み出すことにより、ＩＣカードの認証を可能とした。この場合、クローズドシステムとしての入口発券出口収受方式に適用可能である。

【０１０８】また、第２実施例では、ＩＣカードとＯＢＵとの間の通信路を保護し、ＩＣカード固有の鍵をＯＢＵに安全に転送し、本来のＩＣカードと路側システムとの間で行うべき相互認証のプロトコルのＩＣカードの役割をＯＢＵに代行させ、ＯＢＵと路側システムとの間で高速な伝送処理を可能とした。この場合、オープンシステムの均一路側システムに適用可能である。

【０１０９】

【発明の効果】以上詳述したようにこの発明によれば、ＩＣカードの通信速度が遅く、計算能力が小さくても暗号鍵を用いて無線で相互認証を行って料金の収受を行うことのできる相互認証システムと有料道路の料金収受システムと料金収受システムの相互認証方法を提供することができる。

【図面の簡単な説明】

【図１】この発明の料金収受システムに係るＩＣカード１の構成を示すブロック図。

【図２】ＯＢＵの構成を示すブロック図。

【図３】クローズドシステムに用いられる入口路側システムの構成を示す図。

25

【図４】クローズドシステムに用いられる出口路側システムの構成を示す図。

【図５】オープンシステムに用いられる均一路側システムの構成を示す図。

【図６】通行券自動発行機の構成を示す図。

【図７】出口車線制御装置の構成を示す図。

【図８】ＩＣカードとＯＢＵと路側システムとの間の情報の流れを説明するための図。

【図９】発行局におけるＩＣカード発行時の秘密鍵を示す図。

【図１０】ＯＢＵとＩＣカードとの相互認証動作を説明するための図。

【図１１】発行局におけるＯＢＵ発行時の暗号鍵を示す図。

【図１２】ＯＢＵとＩＣカードとの相互認証動作を説明するための図。

【図１３】メッセージ認証コードを使用した認証システムを説明するための図。

26

【図１４】メッセージ認証コードを使用した相互認証システムを説明するための図。

【符号の説明】

１…ＩＣカード

２…ＯＢＵ（On Board Unit）

１０、２０、３０１、４０１…ＣＰＵ

１１、２１、３０２、４０２…ＲＯＭ

１２、２２、３０３、４０３…ＲＡＭ

１３、２３、３０４、４０４…乱数発生器

１４、２４、３０５、４０５…鍵格納エリア

１５、２５、３０６、４０６…暗号化アルゴリズム実行器

３０…通行券自動発行機

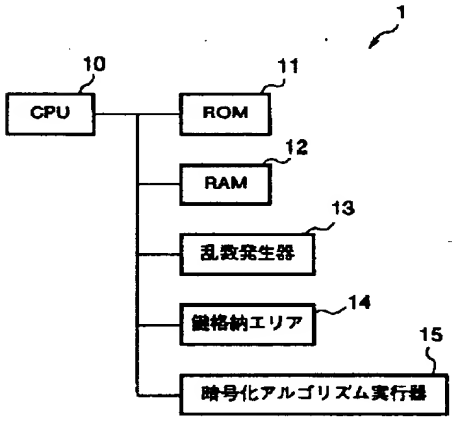
４０…出口車線制御装置

４３…出口ブース内機器

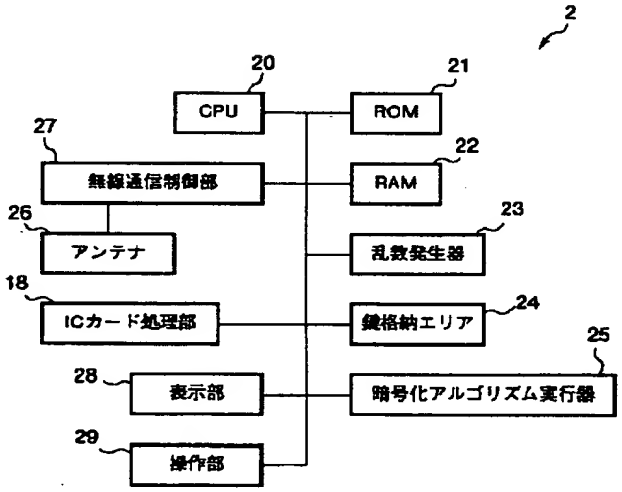
ＲＳＥ…路側システム

ＲＣＣ…ＩＣカード発行局

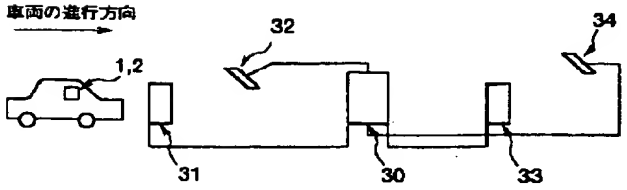
【図１】



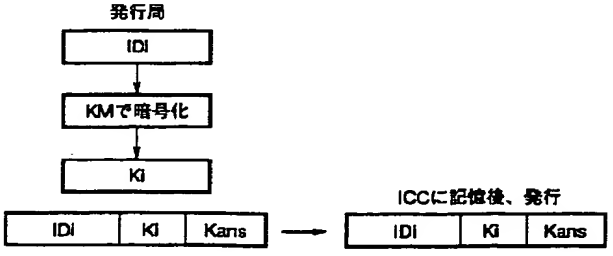
【図２】



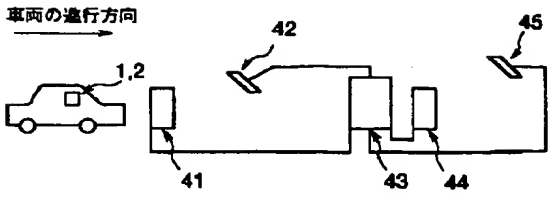
【図３】



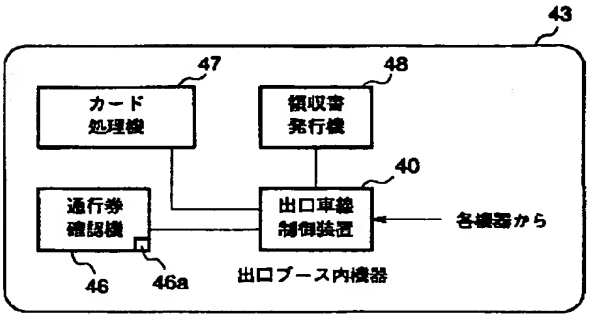
【図９】



【図４】

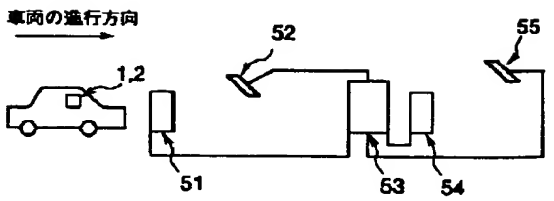


（ａ）

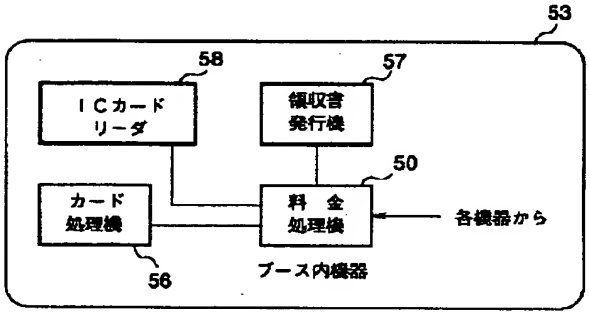


（ｂ）

【図５】

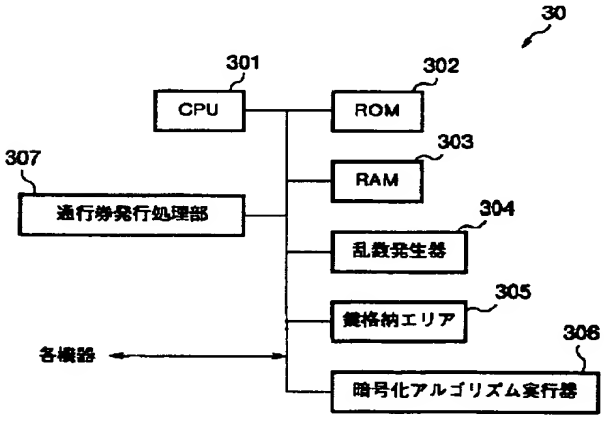


（ａ）

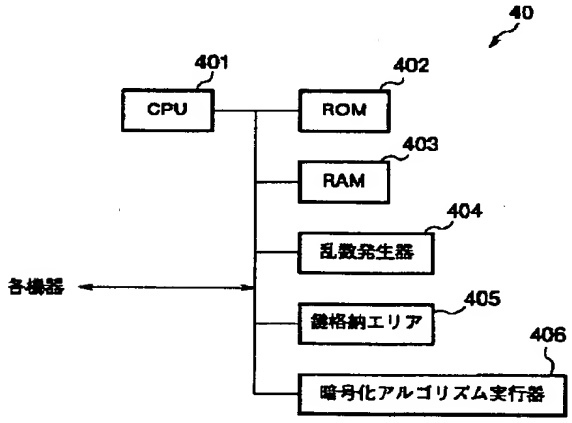


（ｂ）

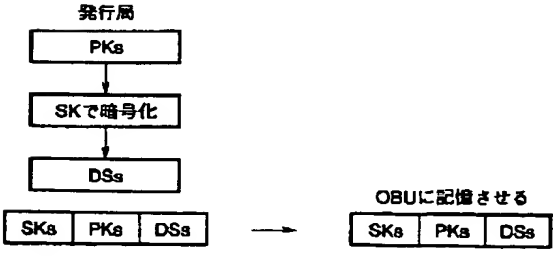
【図６】



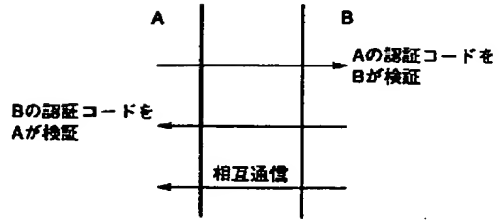
【図７】



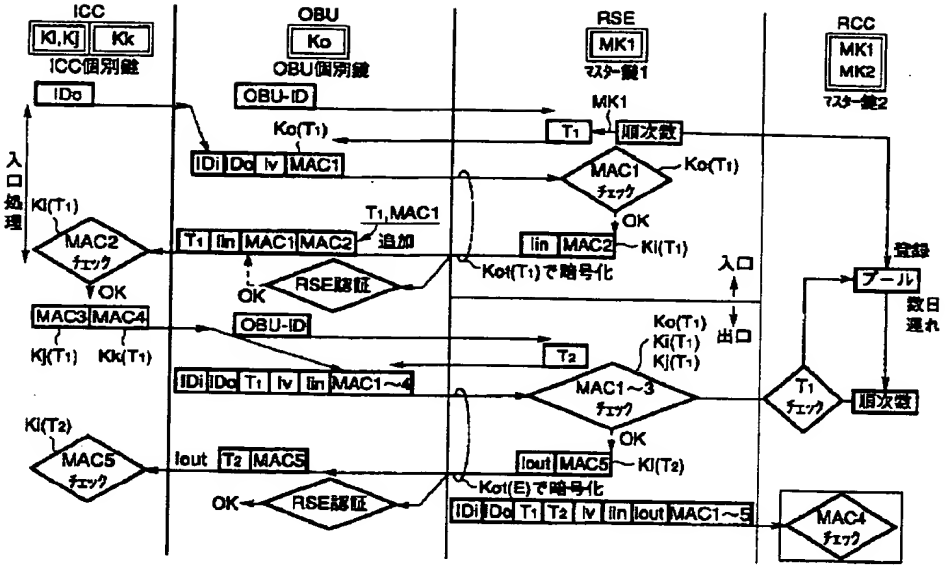
【図１１】



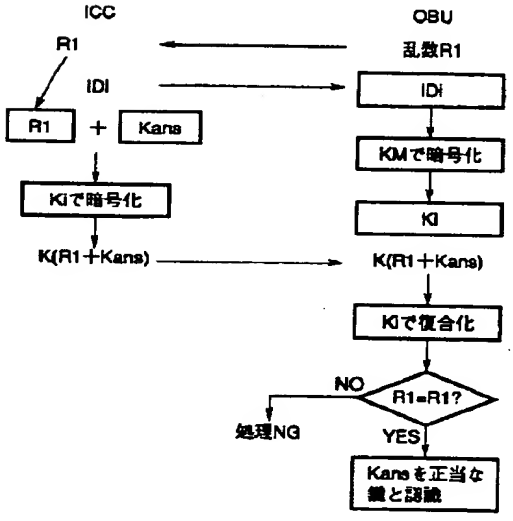
【図１４】



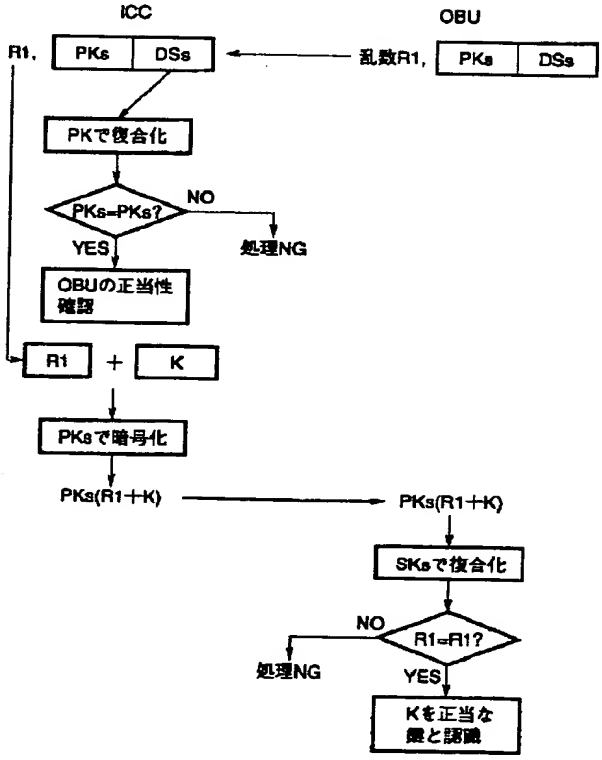
【図８】


ICC
Ki,Kj
Kk
ICC個別鍵
IDo
入口処理
Ki(T1)
MAC2 チェック
OK
MAC3 MAC4
Kj(T1)
Kk(T1)
Ki(T2)
MAC5 チェック
Iout T2 MAC5
OBU
Ko
OBU個別鍵
OBU-ID
Ko(T1)
IDi Do Iv MAC1
T1,MAC1 追加
T1 Iin MAC1 MAC2
RSE認証
OK
OBU-ID
T2
IDi IDo T1 Iv Iin MAC1～4
OK
RSE認証
RSE
MK1
マスター鍵1
MK1
T1
順次数
MAC1 チェック
Ko(T1)
OK
Iin MAC2
Ki(T1)
Ko(T1)で暗号化
入口
出口
Ko(T1)
Ki(T1)
Kj(T1)
MAC1～3 チェック
OK
Iout MAC5
Ki(T2)
Ko(E)で暗号化
IDi IDo T1 T2 Iv Iin Iout MAC1～5
MAC4 チェック
RCC
MK1
MK2
マスター鍵2
T1 チェック
順次数
登録
プール
数日遅れ

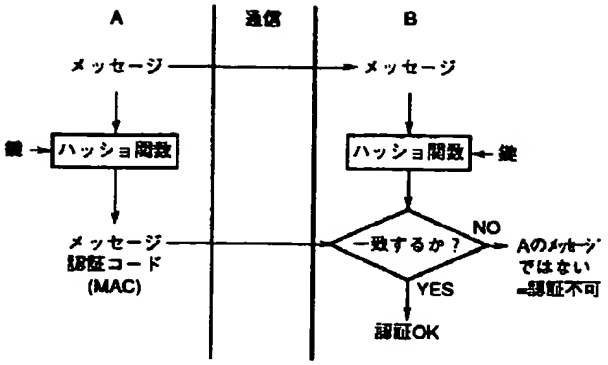
【図１０】


ICC
OBU
R1
乱数R1
IDi
IDi
R1
+
Kans
KMで暗号化
Kiで暗号化
KI
K(R1＋Kans)
K(R1＋Kans)
Kiで復合化
NO
R1=R1?
処理NG
YES
Kansを正当な鍵と認識

【図１２】


ICC
OBU
R1,
PKs
DSs
乱数R1,
PKs
DSs
PKで復合化
PKs=PKs?
NO
処理NG
YES
OBUの正当性確認
R1
+
K
PKsで暗号化
PKs(R1＋K)
PKs(R1＋K)
SKsで復合化
NO
R1=R1?
処理NG
YES
Kを正当な鍵と認識

【図１３】



フロントページの続き

(72) 発明者　内藤　一敏
東京都港区芝浦一丁目１番１号　株式会社
東芝本社事務所内